华为云隐私保护白皮书

版本　　V1.0
发布日期　2019年7月

华为技术有限公司

版权声明©华为技术有限公司2019。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：　　深圳市龙岗区坂田华为总部办公楼　邮编：518129

网址：　　华为　– http://www.huawei.com/cn/, http://e.huawei.com/cn/

　　华为云 – https://intl.huaweicloud.com/

客户服务邮箱：support@huawei.com

客户服务电话：4008302118

引言

随着云计算技术不断更新和云服务的不断演进，越来越多的企业选择使用公有云服务。云服务为企业带来便捷和更丰富的选择，同时也带来了新的机遇和挑战。如何保护云上个人数据的安全引起国家、企业、民众的关注和重视。

2016年欧盟发布《通用数据保护条例》（General Data Protection Regulation，以下简称GDPR）并于2018年5月正式生效，对个人隐私权利提出了明确的法律要求。近年来，阿根廷、新西兰、巴西、印度、土耳其等国家相继制定或修订本国隐私保护法律。全球范围愈加严格的隐私监管态势客观上对隐私保护合规提出更高要求。

华为云在隐私保护方面付出诸多努力并取得了显著的成效，我们希望能够借此白皮书将华为云的隐私保护理念和措施分享给客户，为客户在使用华为云过程中可能遇到的隐私保护相关问题答疑。当然，实现隐私保护需要强大的安全能力为其提供支撑，隐私保护和安全息息相关。华为云在安全方面也具备行业领先的积累和实践，详细内容请查看《华为云安全白皮书》和《华为云数据安全白皮书》。

华为云秉承中立态度，严守服务边界，保障数据为客户所有、为客户所用、为客户创造价值；华为云承诺将确保相关业务遵从业务所在国家/地区适用的隐私保护法律法规。

《华为云安全白皮书》和《华为云数据安全白皮书》：
https://intl.huaweicloud.com/zh-cn/securecenter/overallsafety.html

目录

1. 概述

网络安全和隐私[①]保护一直是华为生存之本，从创立至今，华为人便一直坚定地朝着这个方向不懈努力。华为云始终充分理解隐私的重要性，继承华为公司在隐私保护方面30多年的实践与经验，以及海外170多个国家20多年的实践与经验，现已将网络安全和隐私保护充分融入到每个云服务中，致力于**做尊重和保护客户隐私，客户稳定可靠、安全可信、可持续演进的云伙伴**。华为云郑重对待并积极承担相应责任，矢志不渝地朝着这一愿景不断奋斗。华为云秉承公司以**网络安全和隐私保护为最高纲领，** 围绕此最高纲领为基础，设置专业的隐私保护团队，制定完善流程，积极研发新技术，不断建设华为云隐私保护的能力。

隐私保护的优秀实践依赖全方位以及系统性的体系支撑：华为云以国内外隐私保护的法律法规为基石，参考业界广泛认可的优秀实践，已形成适合华为云的隐私保护体系。华为云投入大量的专业人员和资源支撑新技术的研究和应用以及保障隐私保护体系的有效运转，确保华为云的隐私保护处于行业领先的位置，实现华为云隐私保护的目标：**遵守严格的服务边界，保护客户个人数据安全， 助力客户实现隐私保护。**

本白皮书将带领客户深入了解华为云隐私保护体系、华为云如何保护个人数据[②]以及华为云如何帮助客户实现个人数据安全。

① **隐私**：最广泛的定义是个人let alone的权利。物理上隐私是指个人住宅或个人财产、搜身、监控或提取生物特征信息，而信息性的隐私是指个人控制、编辑、管理和删除关于自己信息的能力和决定如何与他人沟通这些信息的能力。本白皮书主要谈及的是信息性的隐私。

② **个人数据**:个人数据主要指与一个身份已被识别或者身份可被识别的自然人（“数据主体”）相关的任何信息，其主要包括：自然人的email地址、电话号码、生物特征（指纹）、位置数据、IP地址、医疗信息、宗教信仰、社保号、婚姻状态等。

2. 隐私保护责任

华为作为云服务提供商（CSP）向客户提供了基础设施即服务（IaaS），平台即服务（PaaS）和软件即服务（SaaS）各类云服务，在复杂的云服务环境中如何实现隐私安全，需要客户与华为云共同努力。隐私保护对企业提出了明确的要求，本章我们将基于以下责任模型介绍客户在使用云服务时需要承担的隐私保护责任和义务，以及华为云如何帮助你更好的实现隐私安全。

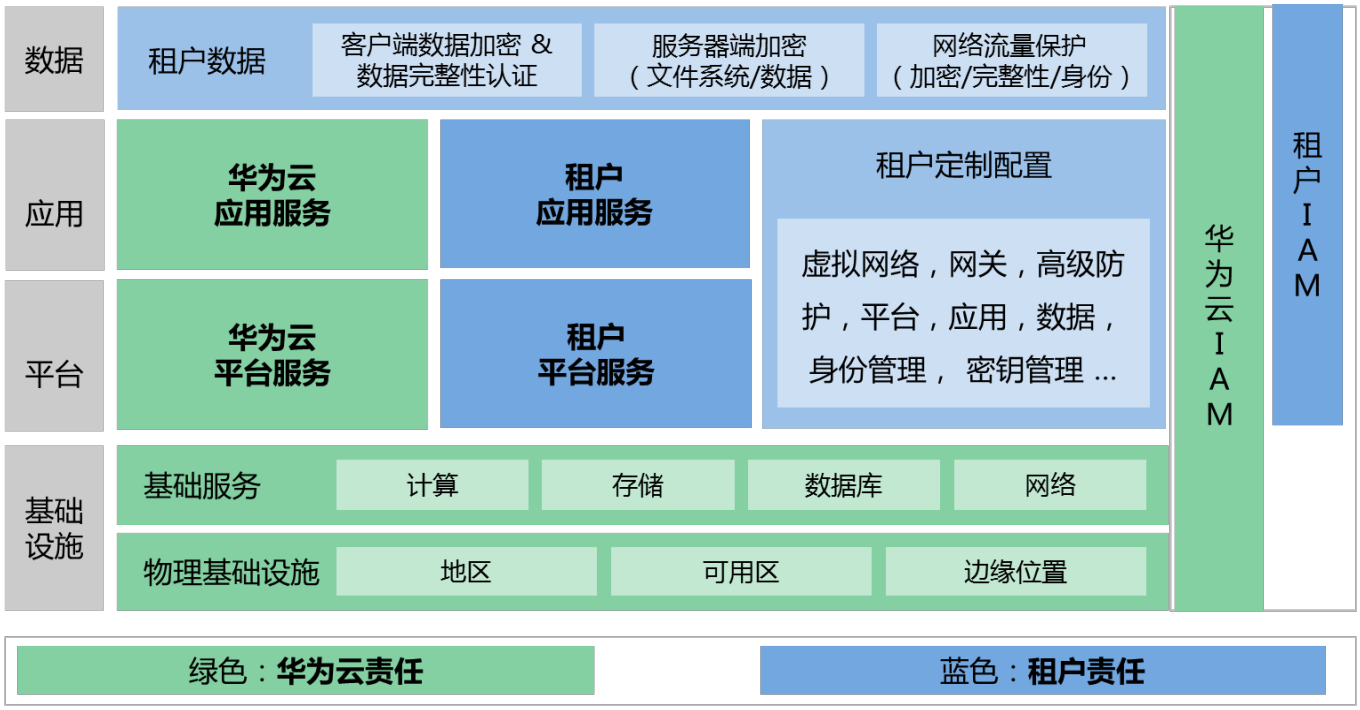


图1：隐私保护责任模型

如上图所示，华为云主要负责云服务自身的安全以及合规，并为客户提供在数据处理、存储、转移等过程中的所需的隐私特性。针对客户内容数据③，客户拥有全部的权利和义务，包括隐私保护的义务，制定安全和隐私保护策略和措施确保个人数据安全，保障数据主体④权利以及各项活动合规。

该模型帮助客户理解华为云和客户各自承担的隐私保护责任和义务，有利于客户识别其个人数据，制定合适的个人数据保护策略，从而最终更好地实现隐私保护。

③ **客户内容数据**：客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

④ **数据主体**：一个身份已被识别或者身份可被识别的自然人。

基于责任模型，华为云与客户主要承担如下的隐私保护责任：

► **华为云的责任：**

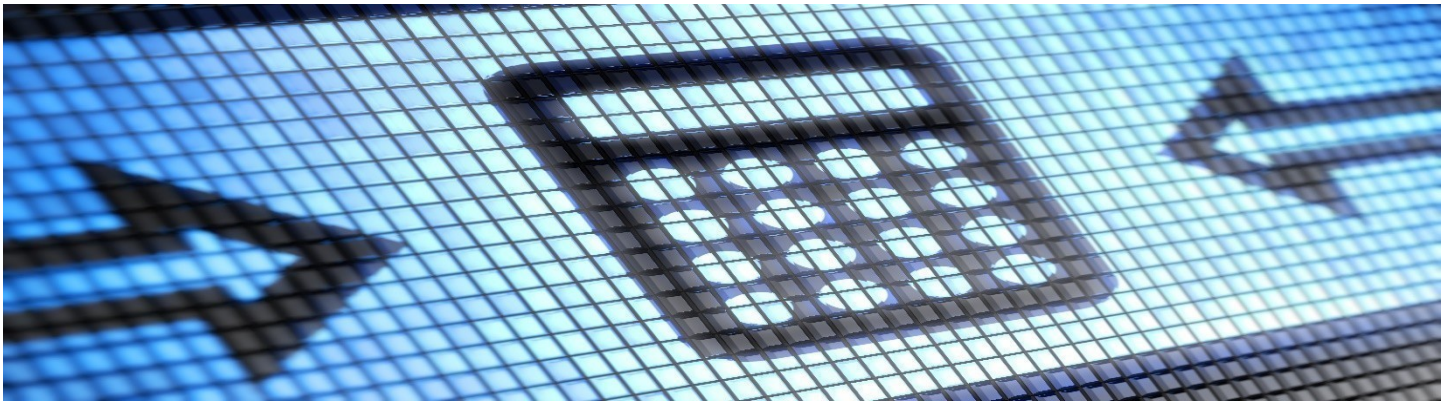
华为云作为云服务提供方，负责构建由基础设施层、平台层、应用层组成的云平台，并负责云平台基础设施如物理环境、软硬件、计算、网络、数据库、存储等以及平台层、应用层的安全。华为云各项活动和云服务遵从隐私保护相关法律法规，为客户提供稳定、安全和有利于隐私保护的云环境。

华为云为客户提供多种隐私保护技术，包括访问控制和身份认证、数据加密、日志和审计和相关的隐私增强技术，以及基于此基础上的华为云各项服务，帮助客户根据业务需求进行隐私保护。华为云拥有完善的隐私保护体系和多方位的隐私保护管控机制，能实现华为云隐私保护的责任。

► **客户的责任：**

客户对其内容数据拥有全面控制权，应正确、全面地识别云端的个人数据，选择恰当的服务并制定安全和隐私保护策略以保护个人数据安全。根据业务和隐私保护的需求进行安全配置工作，例如操作系统配置、网络设置、安全防护、数据库加密策略等，并设置恰当的访问控制策略和密码策略。客户可使用华为云为其提供的多种隐私保护服务，例如使用数据识别技术对数据进行识别和分类、使用访问控制服务对个人数据设置最小权限并按需分配权限、使用加密手段对个人数据的存储和传输进行保护等。

客户应保障其数据主体的权利，响应数据主体请求，当发生个人数据泄露事件时，通知数据主体并采取相应措施。客户可使用华为云为其提供的多种隐私保护服务，例如使用日志功能，保留对个人数据的操作记录，以帮助保障其用户对个人数据的知情权。客户应确保其对个人数据处理符合隐私保护相关法律法规的要求。对此，华为云提供多种隐私保护服务及合规解决方案，帮助客户实现全面的隐私保护合规。



3. 华为云隐私保护体系

华为云建立完善、规范和统一隐私保护体系确保云平台的隐私保护得以实现，并帮助客户实施隐私保护。华为云制定隐私保护七大原则，同时采用业界认可和先进的理念PbD⑤作为指导，结合华为云实际情况形成华为云隐私保护理念。隐私保护理念广泛应用在华为云的组织和人员管理、云平台个人数据安全管理以及为客户提供的隐私服务等各个方面。同时，华为云使用PIA⑥识别隐私风险并采取恰当的方式消除或降低风险。华为云尊重用户的隐私权利，在官网明显处提供清晰的《隐私政策声明》⑦以及客户反馈通道，帮助客户了解华为云隐私保护的信息。

⑤ Privacy by design：隐私融入设计方法（PbD）最早作为针对产品研发周期隐私保护的方法。经过近几年的发展，逐渐演变成隐私保护的管理理念。 PbD提倡**全面、提前、主动**将隐私保护融入业务和各项活动中，帮助组织在隐私保护中取得主动地位。

⑥ Privacy Impact Assessment：隐私影响评估作为业界通用的隐私评估与设计工具被广泛使用和认可。PIA帮助组织识别并减少业务的隐私风险，识别和最小化潜在隐私风险的过程

⑦《隐私政策声明》可通过以下网址访问：https://intl.huaweicloud.com/zh-cn/declaration/sa_prp.html#

3.1 华为云隐私保护基本原则

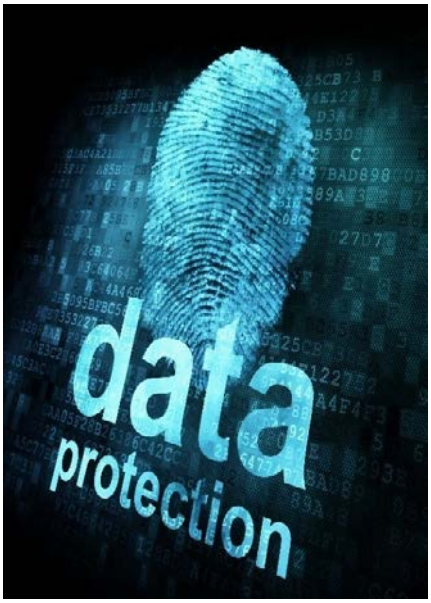
- **合法、正当、透明：**华为云以合法、正当、对数据主体透明的方式处理个人数据。
- **目的限制：**华为云基于具体、明确、合法的目的收集个人数据，不以与此目的不相符的方式做进一步处理。
- **数据最小化：**华为云在处理个人数据时应遵循数据处理目的，且是必要的、适当的。华为云尽可能对个人数据进行匿名或化名处理，降低对数据主体的风险。

- **准确性**：华为云确保个人数据的准确性，并在必要的情况下及时更新。根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人数据。
- **存储期限最小化**：华为云在存储个人数据时不超过实现数据处理目的所必要的期限。
- **完整性与保密性**：华为云根据现有技术能力、实现成本、隐私风险程度和概率采取适度的技术或组织措施确保个人数据的安全，包括防止个人数据被意外或非法损毁、丢失、篡改、未授权访问或披露。
- **可归责**：华为云负责且能够对外展示遵从上述原则。

3.2 组织和人员管理

华为云成立隐私保护组织，以PbD的理念对组织和人员进行管理，并对隐私保护人员执行系统化的隐私能力管理。

隐私保护组织：华为云设置了隐私保护专家团队，包括隐私保护领域专家、法务人员以及网络和信息安全专职人员，为华为云隐私保护战略和实践上提供专业的支撑。在各产品、服务的业务团队中，华为云设置专门的隐私保护角色，负责云服务的隐私保护合规与能力建设。在各个业务所在国家和地区，华为云配备了法务和隐私保护专职人员，帮助华为云在当地开展的各类活动满足适用的隐私法律法规要求。



人员管理：华为云从多方面确保全体员工资质、能力和行为符合隐私保护的需求，要求员工每年应通过隐私保护的相关考核。在此基础上，华为云识别隐私保护相关岗位，明确定义岗位职责。华为云对新员工进行背景调查和技能考核确保员工符合要求；所有员工在职期间需要参加隐私保护意识相关培训，并通过考核。当员工不再负责当前工作时，华为云保证相关权限被删除。

人员技能：华为云通过多种形式的培训定期为全员提供隐私保护意识培训，以加深员工对隐私保护的理解和对华为隐私保护政策规定的了解。对于负责隐私保护相关工作的员工，华为云要求其参加技能培训并通过考核。

3.3 隐私保护流程框架

华为云将隐私保护基本原则全面融入到相关的流程规范中，以规范各项工作的隐私保护管理。华为云建立全面的隐私保护流程体系，通过一系列科学、严格的流程，确保业务活动开展符合隐私保护的要求，如隐私**流程框架**、保护政策、隐私保护设计规范、保障数据主体权利，个人数据留存满足存储期限最小化以及完整性和保密性等原则。

3.4 隐私保护管理工具

华为云使用多种隐私保护平台工具，帮助华为云更快速、系统、高效地处理与隐私保护相关的各项工作。**个人数据自动发现工具，**识别某个系统或者文件里的个人数据，以了解系统或文件是否包含个人数据以及个人数据的类型，可以帮助华为云采取恰当的隐私保护措施。例如，个人数据自动发现工具如扫描出某个文件中有个人数据，华为云可根据识别情况进行加密或在安全通道中流转。**个人数据管理工具**，对华为云各个服务场景包含的个人数据类型、存储的地点，是否涉及跨境转移以及个人数据的流转进行记录，通过此工具，华为云可对各个服务中个人数据的情况进行集中管理，有利于帮助客户了解各类服务中涉及的个人数据类型等。**PIA管理工具**可记录个人数据类型清单，并识别收集个人数据的原因以及目的。使用PIA管理工具还可对相关业务场景进行隐私风险分析和评估，可帮助华为云识别隐私保护风险并制定和实施相应的风险处置措施。

4. 华为云如何保护客户个人数据

华为云对客户的个人数据安全非常重视，在管控机制和技术上采取了先进，严格的管控，确保客户个人数据安全。

4.1 个人数据生命周期管理

为更好的保护个人数据以及保障客户的数据权利，华为云将个人数据生命周期分为七个阶段并实施全生命周期的隐私保护管控，将个人数据生命周期各个阶段的管控要求融入到所有业务流程之中。

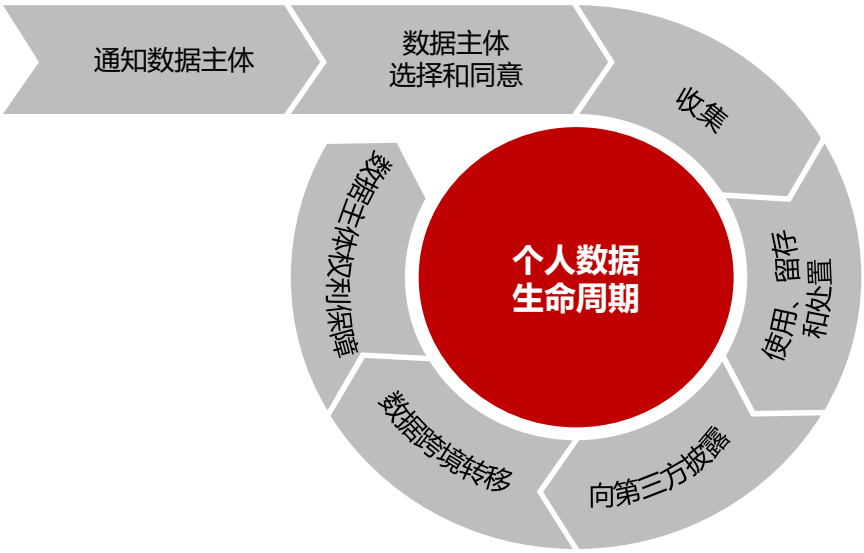


图2: 个人数据生命周期

华为云仅在获得客户的同意后，收集提供服务所必须的客户的个人数据，同时提供隐私通知告知客户所收集的个人数据类型、目的、处理方式、时间等内容。如在官网提供隐私政策声明以及客户同意及撤销同意的机制。对于各类线下市场营销活动中需收集个人数据时，在显著的位置提供隐私通知，并在收集个人数据时提供同意选项。华为云在其官网上提供丰富的配置选项，客户可根据偏好设置接收消息的种类和方式。针对涉及个人数据处理相关特性的云服务，华为云在其产品资料中，告知客户关于个人数据的种类、处理和存储的方式等相关信息，客户可根据产品资料的信息采取相应的隐私保护措施。

华为云对留存在华为云平台上的个人数据，采取严格的管控措施，为了确保个人数据的安全，对个人数据的接入、认证、授权、存储、审计进行统一管理。华为云制定了明确的留存时间，在超出数据处理所需要的时间，个人数据将被自动删除。华为云对运维人员权限实行基于角色的访问控制权限管理，根据岗位需求授予相应的权限并进行定期监控确保访问权限与岗位需求相匹配。华为云定期对日志进行回溯审计，对人员操作行为进行审阅以检查对个人数据操作的合理性和必要性。

华为云对所有供应商按要求进行尽职调查及隐私安全能力评估，合同中明确供应商作为处理者/子处理者的隐私保护义务及适用法律法规的要求，确保供应商满足客户的隐私保护要求。其他华为云可能依法向第三方披露数据的场景可详见《隐私政策声明》。

华为云在全球多个国家建立数据中心，在运营运维过程中涉及需要进行数据跨境传输的场景时，遵循当地隐私保护法律法规并经过内部严格评审。如在签订数据转移协议或获得客户的明确同意之后进行数据跨境转移，保证个人数据将被合法、正当、透明地处理。

华为云配备专业团队响应客户关于个人数据和隐私保护相关的请求，当接收到客户的请求后进行问题处理，并在规定时间内完成请求处理，反馈处理结果给客户。华为云设置7X24小时专业安全事件响应团队，按照适用法律法规要求，对个人数据泄露事件及时披露，同时执行应急预案及恢复流程，以降低对客户的影响。

数据主体权利保障：华为云为客户提供通道，有任何隐私保护相关的请求，可通过hws_security@huawei.com联系我们。

4.2 个人数据保护安全技术

- **针对客户个人数据**

使用**访问控制和身份认证技术**管理访问个人数据的权限控制。华为云按照最低所需原则，根据不同职位职责定义并管理不同访问权限，员工仅拥有职位所需的最低的权限，并在不需要时立刻删除。华为云制定严格的密码策略和启用多因素认证，对访问个人数据的权限进行严格控制。

华为云广泛采用**加密技术**对客户个人数据进行加密存储和传输，确保个人数据存储和传输中的安全。

通过**日志记录和审计技术**记录对各关键系统的访问和操作和对密钥的使用等，定时进行监控和审计，及时发现和纠正隐私保护方面可能存在的不合适行为；同时分析潜在的隐私保护和个人数据安全隐患以便及时迅速的做出反馈，解决问题。

- **针对客户的内容数据**

华为云使用各种数据安全技术和相关管控措施如身份认证和访问控制、数据传输及存储加密技术、日志记录等手段保障华为云服务自身的安全性，并向客户提供丰富的安全服务以满足租户不同安全级别的要求，详情可参考华为云已发布的《华为云数据安全白皮书》。

4.3 隐私增强技术

华为云研究团队同时致力研发各类**隐私增强技术（PET）**,积累隐私保护工程技术能力，以满足客户不同需要实施隐私保护。华为云现已拥有的一系列PET,包括等价类匿名、差分隐私、防跟踪技术、区块链私人支付以及隐私保存计算等。

- **数据屏蔽**

华为云的数据屏蔽技术通过包括**掩码、加噪、枚举、截断、哈希、标志化**等手段，防止从数据中关联用户身份及敏感信息，对个人数据的单个字符的屏蔽来保护数据隐私，降低数据泄露的风险。

- **差分隐私**

差分隐私是一种加噪算法，在保留数据一定的可用性，又能保证攻击者无法推断出某个用户的信息。 差分隐私在不知道数据库本身内容的情况下，注入**“噪声”**。从而数据集进行模糊化处理，但不影响统计结果。可在数据库查询时，减少个人数据被识别的几率。

- **可搜索加密**

可搜索加密技术可实现对加密状态下的个人数据进行搜索，如客户的邮箱、电话号码、身份证号等加密存储的个人数据，可以在不明文显示的情况下进行搜索处理，降低个人数据泄露风险。

5. 华为云如何帮助客户实现个人数据安全

华为云深刻理解保护个人数据对客户的重要性，并努力地采取管控措施和提供相应的服务帮助客户保护其个人数据安全。

5.1 云服务生命周期的隐私管控

为保证提供给客户的云服务符合合规要求并具备隐私保护的特性，华为云基于PbD理念，在云服务生命周期的每个阶段都将隐私保护要求放在首位，在每个关键节点采取严格的隐私保护管控要求，以确保和提高云服务隐私保护合规性和保障个人数据安全的能力，充分满足客户隐私保护的需求，帮助客户保护其用户的隐私。

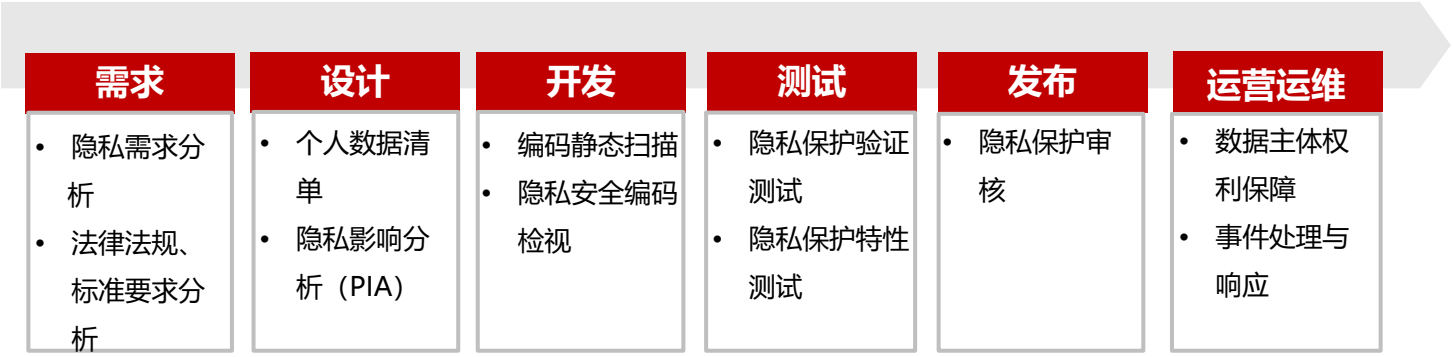


图3: 云服务生命周期及隐私管控

华为云服务从需求设计到运营运维整个生命周期全过程执行隐私保护管控。需求分析过程中对隐私需求和相关法律法规分析，将安全和隐私需求优先纳入服务规划中。设计阶段梳理涉及的所有个人数据类型并记录，通过PIA方法识别潜在风险并将风险控制措施融入到服务设计中。开发阶段通过编码静态扫描及隐私安全编码检视，确保开发过程及编码符合公司相关的开发规范。在测试阶段，所有隐私特性需通过严格测试并经过专家团队审视，确保隐私需求和设计在云服务中实现。云服务隐私保护合规不仅限于研发阶段，在服务持续运维运营阶段，华为云通过各项技术和管理措施保证个人数据不被非授权访问和处理，保障数据主体权利，确保云服务持续的隐私安全。

华为云在每个云服务生命周期采取的隐私保护管控措施，以实现：

- 全生命周期贯彻PbD的理念，使每个云服务本身满足隐私合规要求，同时具有隐私保护特性。
- 严格测试和审查，确保隐私合规需求得到实现、隐私保护特性的有效。
- 对隐私保护的要求不止步于产品上线，在运营运维的阶段，通过人员及流程的管控，为客户提供合规的云服务，帮助客户实现其隐私保护。

5.2 隐私保护服务能力

华为云将技术上的丰富积累和新技术的研发成果融入到华为云服务当中，为客户提供基础的安全和隐私保护的服务帮助客户保护个人数据。

华为云提供多种数据安全和隐私保护的服务，更多华为云服务，可访问华以下产品页面获取：

https://intl.huaweicloud.com/zh-cn/product/

统一身份认证服务

统一身份认证服务（IAM）是华为云为客户提供适合企业的用户管理、身份认证和细粒度的云上资源访问控制服务。

数据加密服务

数据加密服务（DEW）支持客户对存储到数据库的个人数据进行加密并对密钥进行统一管理以增强个人数据安全。

监控和日志审计服务

华为云各服务提供基本的日志记录功能，客户可通过云服务内嵌的功能对进行日志记录配置。同时华为云提供集中、完整的日志记录和审计服务： 华为云的云日志服务（LTS）和云审计服务（CTS）。

数据库安全服务（DBSS）

DBSS帮助客户发现存储在各类数据库中的个人数据及敏感数据，并进行相应的数据保护处理。

数据检测服务

全球首个结构化数据检测服务。具备结构化数据检测及非结构化敏感数据检测特性，用户可快速从自己拥有的海量数据中迅速识别出敏感数据，满足GDPR等合规要求，可识别出不合规的分析报告。帮助客户快速构建隐私合规能力。

6. 隐私保护合规与认证

华为云遵守业务开展地所有适用的隐私相关法律法规。华为云投入专业的法律团队，紧密关注法律法规更新情况，对海内外法律法规保持持续跟踪并进行快速分析，确保遵循法律法规的要求。

华为云隐私保护和个人数据安全的能力和成效在全球范围得到广泛认可第三方认证，截至目前为止，华为云共取得海内外十余家机构的相关认证，其中包括：**ISO27001、ISO27018、 ISO27017 、SOC2审计 、PCI DSS认证（针对信用卡数据） 、CSA STAR 金牌认证、国际通用准则 CC+EAL3+、 网络安全等级保护三级（中国）、可信云服务认证（中国） 、云服务用户数据保护能力（中国）**、MTCS Level 3（**新加坡**）等。

华为云积极关注业界权威隐私认证机制的出台，并持续提高要求，完善隐私保护体系，增加和更新安全和隐私方面的认证。同时，华为云和隐私保护相关协会紧密合作，对隐私保护前沿资讯及技术进行探讨，帮助华为云打造一个可持续发展的、安全的隐私保护环境。

华为云与客户共同承担合规责任，如客户需要进行合规性认证，可以从华为云获得必要的协助，华为云相关认证资质证明可在华为云信任中心获取：https://intl.huaweicloud.com/zh-cn/securecenter/safetycompliance.html

7. 结语

华为云在海内外的业务日渐壮大，为客户提供智能、安全、可信的云服务面临更多、更高要求。华为云始终秉持华为公司**“以客户为中心”**的核心价值观，充分理解客户个人数据安全的重要性，尊重和保护客户隐私权利；华为云具备业界领先的安全及隐私保护技术，并通过云服务和解决方案的方式向客户提供相关能力，帮助客户轻松应对日益复杂和开放的网络环境及日趋严格的隐私保护法律法规要求。

秉承公司的最高纲领，华为云在隐私保护实践中将继续践行隐私保护愿景和目标，并持续加大投入，不断提升能力为客户提供安全可靠的云平台和隐私保护技术帮助客户保护个人数据。华为云始终保持开放态度，不断研究学习、与多方合作，吸长补短，持续提升和丰富华为云安全和隐私保护服务，帮助客户创造价值。

华为云希望借此白皮书的发布，分享在隐私保护的实践和经验，也希望能与客户继续并肩同行，共同创造安全、可信、透明的云环境。

更多关于华为云隐私保护内容和相关服务，可访问华为云官网：

https://intl.huaweicloud.com/zh-cn/